[67] K. Pohl, G. Böckle, and F. van der Linden, *Software Product Line Engineering - Foundations, Principles, and Techniques.* Springer, 2005.

[68] S. Sidiroglou-Douskos, S. Misailovic, H. Hoffmann, and M. C. Rinard, "Managing Performance vs. Accuracy Trade-offs With Loop Perforation," in *SIGSOFT/FSE'11 19th ACM SIGSOFT Symposium on the Foundations of Software Engineering (FSE-19) and ESEC'11: 13th European Software Engineering Conference (ESEC-13)*, pp. 124–134, 2011.

[69] Avizienis and Kelly, "Fault Tolerance by Design Diversity: Concepts and Experiments," *Computer*, vol. 17, no. 8, pp. 67–80, 1984.

[70] T. Y. Chen, F. Kuo, R. G. Merkel, and T. H. Tse, "Adaptive Random Testing: The ART of test case diversity," *J. Syst. Softw.*, vol. 83, no. 1, pp. 60–66, 2010.

[71] T. Jackson, *On the Design, Implications, and Effects of Implementing Software Diversity for Security.* PhD thesis, University of California, Irvine, 2012.

[72] G. R. Lundquist, V. Mohan, and K. W. Hamlen, "Searching for Software0 Diversity: Attaining Artificial Diversity through Program Synthesis," in *Proceedings of the 2016 New Security Paradigms Workshop*, NSPW '16, (New York, NY, USA), p. 80–91, Association for Computing Machinery, 2016.

[73] P. Koopman and J. DeVale, "Comparing the robustness of posix operating systems," in *Digest of Papers. Twenty-Ninth Annual International Symposium on Fault-Tolerant Computing (Cat. No.99CB36352)*, pp. 30–37, 1999.

[74] I. Gashi, P. Popov, and L. Strigini, "Fault diversity among off-the-shelf sql database servers," in *Proceedings of the 2004 International Conference on Dependable Systems and Networks*, DSN '04, (USA), p. 389, IEEE Computer Society, 2004.

[75] J. C. Knight and N. G. Leveson, "An experimental evaluation of the assumption of independence in multiversion programming," *IEEE Transactions on Software Engineering*, vol. SE-12, no. 1, pp. 96–109, 1986.

[76] B. Randell, "System Structure for Software Fault Tolerance," *SIGPLAN Not.*, vol. 10, p. 437–449, apr 1975.

[77] N. Harrand, *Software Diversity for Third-Party Dependencies.* PhD thesis, Royal Institute of Technology, Stockholm, Sweden, 2022.

[78] J. V. Cleemput, B. Coppens, and B. D. Sutter, "Compiler Mitigations for Time Attacks on Modern X86 Processors," *ACM Trans. Archit. Code Optim.*, vol. 8, no. 4, pp. 23:1–23:20, 2012.

[79] A. Homescu, S. Neisius, P. Larsen, S. Brunthaler, and M. Franz, "Profile-guided Automated Software Diversity," in *Proceedings of the 2013 IEEE/ACM International Symposium on Code Generation and Optimization, CGO 2013, Shenzhen, China, February 23-27, 2013*, pp. 23:1–23:11, IEEE Computer Society, 2013.

[80] S. Bhatkar, D. C. DuVarney, and R. Sekar, "Address Obfuscation: An Efficient Approach to Combat a Board Range of Memory Error Exploits," in *Proceedings of the USENIX Security Symposium*, 2003.

[81] S. Bhatkar and D. C. DuVarney, "Efficient Techniques for Comprehensive Protection from Memory Error Exploits," in *Proceedings of the 14th USENIX*, 2005.

[82] K. Pettis and R. C. Hansen, "Profile Guided Code Positioning," in *Proceedings of the ACM SIGPLAN'90 Conference on Programming Language Design and Implementation (PLDI)*, pp. 16–27, 1990.

[83] S. Crane, A. Homescu, S. Brunthaler, P. Larsen, and M. Franz, "Thwarting Cache Side-channel Attacks Through Dynamic Software Diversity," in *22nd Annual Network and Distributed System Security Symposium, NDSS 2015, San Diego, California, USA, February 8-11, 2015*, The Internet Society, 2015.

[84] A. Romano, D. Lehmann, M. Pradel, and W. Wang, "Wobfuscator: Obfuscating JavaScript Malware via Opportunistic Translation to WebAssembly," in *2022 2022 IEEE Symposium on Security and Privacy (SP) (SP)*, (Los Alamitos, CA, USA), pp. 1101–1116, IEEE Computer Society, may 2022.

[85] M. T. Aga and T. M. Austin, "Smokestack: Thwarting DOP Attacks with Runtime Stack Layout Randomization," in *IEEE/ACM International Symposium on Code Generation and Optimization, CGO*, pp. 26–36, 2019.

[86] S. Lee, H. Kang, J. Jang, and B. B. Kang, "SaVioR: Thwarting Stack-based Memory Safety Violations by Randomizing Stack Layout," *IEEE Trans. Dependable Secur. Comput.*, vol. 19, no. 4, pp. 2559–2575, 2022.

[87] Y. Younan, D. Pozza, F. Piessens, and W. Joosen, "Extended Protection against Stack Smashing Attacks without Performance Loss," in *22nd Annual Computer Security Applications Conference (ACSAC 2006), 11-15 December 2006, Miami Beach, Florida, USA*, pp. 429–438, IEEE Computer Society, 2006.

[88] Y. Xu, Y. Solihin, and X. Shen, "MERR: Improving Security of Persistent Memory Objects via Efficient Memory Exposure Reduction and Randomization," in *ASPLOS '20: Architectural Support for Programming Languages and Operating Systems*, pp. 987–1000, 2020.